ELECTRONIC TENDER SYSTEM

Background of the Invention:

The present invention relates to an electronic tender system, and particularly a method for coding the bidding price and a method for deciding the contract price.

As known from Japanese Patent Laid-Open No.HEI2-118876, for example, such electronic tender system adopts a coding technology, because the bidding price information should be kept secret generally until the tender opening. The coded bidding price information is decoded all at once at the tender opening, to decide the highest or the lowest bidding price among them as the contract price. There, th announcement of all bidding prices allows to everyone to confirm that the contact price has been decided correctly, in other words, it was the highest or the lowest price among th bidding prices.

Recently, it is demanded not to publish the bidding price not accepted as the contact price, in view of the privacy protection. To meet this requirement, for example, an approach has been disclosed in an article, "Multi-round Anonymous Auction Protocols" by Kikuchi, Harkavy and Tyger, published in "IEEE Workshop on Dependable and Real-time E-Commerce System". This approach disclosed in the prior art literature is shown in Fig. 1.

In this approach, the bidder creates a data row corresponding to his bidding price and encodes each data respectively. The opener receives code string data transmitted

by all bidders, integrates and then decodes them to decide the contract price. In this approach, as the code string data of individual bidder is not decoded, the bidding price of respective bidder can be kept secret, and at the same time, the identification information of the highest price bidder can be extracted, by integrating code string data of all bidders.

Now, the principle of identification extraction will be described. A bidder having an identification information IDi, creates a data row corresponding to his bidding price as follows. Suppose the tender reception range be (a, b) and his bidding price a + v (<b), then (v + 1) times x ID_I are enumerated. Next, 0 are enumerated b - (a + v) times. Thus, a data row containing (b - a + 1) elements is generated.

A data row where respective elements of the data row are added by each element is output, by integrating data rows from all bidders generated in this way. In this data row, suppose the element where 0 appears first be t th, the highest bidding price (contract price) is a + t -1, and the bidder who has the identification information indicated by the price of the t – 1st element.

However, in this prior art, the bidding data becomes longer in proportion to the tender reception price range, because the data row is created in proportion to the length of the tender reception range, and then it is divided to code. Further, when a plurality of bidders have offered the contract price, it is impossible to determine th identification r the number of concerned bidders, because the decoding result f the t – 1st element is the sum of ID information of bidders of

the corresponding bidding price.

Summary of the Invention:

It is therefore an object of the present invention to provide an electronic tender system, allowing to reduce the bidding data, and at the same time, to identify the concerned bidder even when a plurality of bidders have offered the contract price, and moreover, to keep secret the bidding information of other bidding prices than that of the successful bidder.

Other objects of the present invention will become clear as the description proceeds.

The electronic tender system according to the present invention is characterized by that a code parameter depending on the bidding price is delivered to the coding function section in its bidder sub-system, and, a contract price candidate selection function, and a retrieve function by the decode parameter depending on the candidate price are provided, in order to decide the contract price in its tender opening sub-system.

The introduction of these code parameter and decode parameter realizes an effect to judge only if the bidding price is identical to the contract price candidate. Therefore, the highest or the lowest bidding price and its bidder can be decided, by judging if there is a bidding price identical to th contract price candidate, changing the contract price candidate one by one from the tender possible highest price or the lowest price, and further, how the other bidders have tend red can be concealed.

Brief Description of the Drawings:

Fig. 1 is a block diagram for showing a conventional method;

Fig. 2 is a block diagram for showing a composition of the present invention; and

Fig. 3 is a block diagram for showing a composition of the retrieve means of the present invention.

Detailed Description of the Preferred Embodiments:

Referring now to Figs. 2 and 3, description will proceed to an electronic tender system according to a preferred embodiment of the present invention.

Fig. 2 is a block diagram showing an embodiment of the present invention. The electronic tender system according to the present invention comprises a bidder sub-system 100 and a tender opening sub-system 200. The bidder sub-system 100 includes a code parameter acquisition means 101and a coding means 102, while the tender opening sub-system 200 includes a reception means 201, a contract price candidate selection means 202, a decode parameter acquisition means 203 and a retrieve means 204.

The retrieve means 204 includes, as shown in Fig. 3, a decoding means 205 and a judgement means 206, and the decoding means 205 decodes sequentially coded bidding prices received by the reception means 201 based on the decode parameter acquired by the decode parameter acquisition means 205, while the judgement means 206 judges that th coded bidding price is identical to the contact price candidate selected by the s lection means 202, in the case when the

decoding result by the decoding means 205 becomes a fixed value.

Note that, in this embodiment, to simplify the description, it is supposed, hereinafter, that a bidder sub-system that has offered the highest price, among bid prices, will be decided as the successful bidder, though it is similar in the case where the lowest price will be the contract price.

The input to the bidder sub-system 100, is the bidding price desired by this the bidder sub-system. The bidding price bid in this bidder sub-system 100 is delivered to the code parameter acquisition means 101. In the code parameter acquisition means 101, the code parameter necessary for the coding means 102 depending on this bidding price is acquired and delivered to the coding means 102. The coding means 102 performs the coding operation based on the supplied code parameter, and delivers the coded bidding data to the transmission means 103. The transmission means 103, transmits the coded bidding data to the reception means 201 of the tender opening sub-system 200.

The reception means 201 of the tender opening sub-system 200, receives the coded bidding data sent from respective bidder sub-system 100, directs the contract price selection means 202 to start the tender opening on the tender opening day. The contract price selection means 202 directed to open the tender, first, takes the highest price within the acceptable range the candidate price, and supplied the decode parameter acquisition means 203 with this candidate price.

The decode parameter acquisition means 203, acquires

this decode parameter depending on this candidate price, and delivers to the retrieve means 204. The retrieve means 204, decodes all coded bidding data received using the supplied decode parameter, in the decoding means 205, and retrieves if there is a bidding price same as the candidate price among the coded bidding data by the judgement means 206. If it is the case, the bidder sub-system that has sent that coded bidding data will be accepted. If there is no coded bidding data created taking this candidate price as bidding price, the retrieve means 204, outputs that the concerned candidate price is not the contract price to the contract price selection means 202.

Upon the reception of a non candidate signal from th retrieve means 204, the contract price selection means 202, takes the next lower price than the current candidate price as a new candidate price, and delivers it to the decode parameter acquisition means 203. Then, the similar operation will be repeated until the judging means 206 decides a successful bidder, or the candidate price becomes lower than the tend r possible range. If the candidate price becomes lower than the tender possible range, it is judged that no bidding is accepted, and this result is output before terminating the processing.

Now, as an example of this embodiment, the case where El Gamal code is used as coding function will be described. Th El Gamal code being well known by those skilled in the art and irrelevant to the present invention, its detailed explanation will be omitted.

First, the tender opening system creates a large prime p and a generator g. Besides, it decides a secret key x (v), a

public key y (v) and a constant M (v) for respective bidding price v. Here, the secret key x (v) and the public key y (v) present the following relation. M (v) may be an arbitrary value, and for example, v and its hash value can be linked as M (v), or it well may be a constant independent of v. As code parameters, M (v) and y (v) are adopted and as decode parameter x (v). The code parameters are published, while the decode parameters are severely controlled in the tender opening sub-system.

The bidder sub-system 100, obtains code parameters, M (v) and y (v), for a bidding price v it desires, and codes M (v) with the public key y (v) based on the El Gamal code. The El Gamal code, belonging to the code type called probabilistic encryption, is known to produce a different coded message even if the same M (v) is coded. The bidder sub-system 100, send this coding result to the tender opening system 200 as coded bidding data C (v).

The tender opening sub-system 200 obtains a decode parameter x (v') for a contract price candidate v' and decodes C (v) using this decode parameter as secret key. There, if v = v', obviously the decoding result will be M(v) = M (v'). On the contrary, if v $\neq$ v', the decoding result will hardly be M(v'). Thus, without obtaining the bidding price, it can be judged if it is equal to the contract price candidate.

If the contract price is decided to be v, all offered code bidding prices, and the decode parameter x (v) corresponding the bidding possible price equal to or larger than v are published by the announcement means. Theref re, everyone can verify that there was no bidding price larger than v and

who has bid the contract price, as they can try to decode all offered code bidding prices using this announced decode parameter.

On the other hand, bidding prices inferior to th contract price can be concealed, as the decode parameter x (v) corresponding to the bidding prices inferior to the contract price is not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding sub-systems have offered the contract price.

As a specific embodiment, now a case where RSA code is used for coding function will be described. The detailed description of RSA code will be omitted as it is well known by those skilled in the art and not relevant to the present invention. For RSA coding, code parameter y (v) is generated automatically form the bidding price v, without table lookup, and moreover, the fixed value M (v) to be coded may not be fixed for all bidders.

First, the tender opening system generates large primes p and q, and supposes n their product. The bidder sub-system generates as follows the code parameter M (v), y (v), for the bidding price v it wishes. That it to say, it generates random numbers, and makes M (v) be the concatenation of v, and this random number, and the hash value where they are coupled. Next, supposing y (v), 1 is concatenated with the hash value of v, making it prime to (p-1)(q-1) each oth r.

Then, M (v) is codifi d with the public key y (v) based on

RSA code of the modulus n. In this case, as different random numbers are generated for respective bidder, different coded messages are generated even if a same v is coded. The bidder sub-system transmits this coding result to the tender opening system 200 as coded bidding data C (v).

The tender opening system 200 calculates y (v') for a contract price candidate v', namely it hash value, and calculates x (v') that is the inverse element of y (v') in the modulus (p-1)(q-1), as decode parameter. Then, C (v) is decoded in the modulus n taking this code parameter as secret key.

Here, if v = v', obviously, the decoding result M (v') will be a correct format by v' and a certain random number. On the other hand, if v $\neq$ v', the decoding result will hardly be such format. Thus, without obtaining the bidding price it-self, it can be judged if it is equal to the contract price candidate.

If the contract price is decided to be v, all offered code bidding prices, and respective result of decoding by the decode parameter x (v) corresponding the tender possible price equal to or larger than v are published by the announcement means. Therefore, everyone can verify that there was no bidding price larger than v and who has bid the contract price, as they can confirm that the result coded by the code parameter y (v') corresponding to the contact price candidate is equal to offered respective code bidding prices, using this announced decode parameter.

On the other hand, bidding prices inferior to the contract price can be concealed, as the decoding result

corresponding to the bidding prices inferior to the contract price is not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding sub-systems have offered the contract price.

Moreover, it is assured that code bidding prices to be input into the tender opening system excludes those outside the bidding period, by publishing code bidding prices received before the bidding deadline, and opening only those published ones. As it is irrelevant to the present invention, the detailed description thereof will be omitted.

Additionally, it can be assured that the tender opening system will not decode illegally the code bidding price, by controlling or generating the decode parameter with a plurality of sub-systems, using distributed secret or group decryption technology or the like. As it is also irrelevant to the present invention, the detailed description thereof will be omitted.

Beside, a digital signature of the code bidding price can be added, in order to prevent the bidder bidding in the name of the other, or denying later the transmitted code bidding price; however, as it is also irrelevant to the present invention, the detailed description thereof will be omitted.

In this embodiment, to simplify, the case where a bidding sub-system that has offer d the highest price, among bid prices, will be decided as the successful bidder has been described in detail; however, similarly, it can easily be applied

to the case wherein the lowest price will be the contract price, or to the case wherein a plurality of bidding sub-system that have offered a bidding price close to the highest price or the lowest price.

It is to be understood that the present invention is not limited to the aforementioned respective embodiments, and obviously, the respective embodiments can be executed by conveniently modifying them, without departing from the technical concept of the present invention.

As described hereinbefore, according to the present invention, it is possible to provide an electronic tender system, allowing to select the bidder who has offered the highest or the lowest price as successful bidder and moreover, to keep secret the bidding information of other bidding prices than that of the successful bidder, based on a basic composition wherein the bidder sub-system codes by means of a code parameter depending on the bidding price, and the tender opening system decodes by a decode parameter depending on the contract price candidate.